

AMENDMENTS TO THE SPECIFICATION

On page 1, before the first paragraph, the following headings and paragraph are inserted:

BACKGROUND

A. Field

This invention relates to secure authentication of a user of a portable data carrier communicating with a terminal.

On page 1, the first paragraph is amended to read:

This invention starts out from a method exemplified, for example, by the method according to ~~the species of the main claim~~. Such a method is known for example from "Handbuch der Chipkarten" (herein-after "Chip card manual"), W. Rankl, W. Effing, 3rd edition, 1999, pp. 692 to 703, under the title "Digital signature". For performing a legally binding electronic signature, a digital signature card containing a secret signature key is accordingly to be used. A signature is performed on a suitable terminal from which the card receives in electronic form a document to be signed. To be able to perform a signature, the user of the card must establish proof of his identity through the terminal. This proof is regularly furnished by entering a PIN (person identification number) which is compared with a reference PIN stored in the card. In future it is planned to perform user authentication by checking a biometric feature, e.g. a fingerprint. When an electronic document has been signed with the help of a signature card after successful authentication of the user, the document can then be passed on in any way. The electronic signature makes it possible to effect particularly security-critical transactions, e.g. the placing of service orders involving costs, by electronic channels.

On page 1, the last paragraph is deleted.

On page 2, before the third paragraph, the following heading is inserted:

SUMMARY

On page 2, before the fifth paragraph, the following heading is inserted:

DESCRIPTION OF THE DRAWINGS